



CVE-2010-3310

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-3310
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-29 17:00:00 UTC
Updated	2023-02-13 04:23:00 UTC
Description	Multiple integer signedness errors in net/rose/af_rose.c in the Linux kernel before 2.6.36-rc5-next-20100923 allow local use

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc3	All	All

Operating System	Linux	Linux Kernel	2.6.36	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc4	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References						
Reference	Source	Link	Tags			
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S	SUSE	lists.opensuse.org	Mailing Lis			
git.kernel.org	CONFIRM	git.kernel.org	Vendor Ac			
SUSE update for kernel - Advisories - Community	SECUNIA	secunia.com	Third Part			
Linux Kernel Multiple Vulnerabilities - Advisories - Community	SECUNIA	secunia.com	Third Part			
'[PATCH] rose: Fix signedness issues wrt. digi count.' - MARC	MLIST	marc.info	Mailing Lis			
oss-security - Re: CVE request: kernel: Heap corruption in ROSE	MLIST	www.openwall.com	Mailing Lis			
git.kernel.org	MISC	git.kernel.org				
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Third Part			
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org	Mailing Lis			
68163	OSVDB	www.osvdb.org	Broken Lir			
USN-1000-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Part			
Linux Kernel Rose Protocol 'rose_ndigis' Heap Memory Corruption Vulnerability	BID	www.securityfocus.com	Third Part			
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	Third Part			
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org	Mailing Lis			
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org	Mailing Lis			
mandriva.com	MANDRIVA	www.mandriva.com	Third Part			
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org	Mailing Lis			
oss-security - CVE request: kernel: Heap corruption in ROSE	MLIST	www.openwall.com	Mailing Lis			
404: File not found	CONFIRM	www.kernel.org	Patch, Ver			
Debian -- Security Information -- DSA-2126-1 linux-2.6	DEBIAN	www.debian.org	Third Part			
mandriva.com	MANDRIVA	www.mandriva.com	Third Part			
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Third Part			
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org	Mailing Lis			
CVE Program record	CVE.ORG	www.cve.org	canonical			
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,			

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)